

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT
☐ SUPERSEDING

OFFENSE CHARGED

Count One: 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B), and 2 – Obtaining Information from a Protected Computer ☐ Petty
 Count Two: 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2 – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer ☐ Minor
 Count Three: 18 U.S.C. §§ 1030(a)(7)(A), (a)(7)(B), (a)(7)(C), and (c)(3)(A), and 2 – Extortion Involving Computers ☒ Misdemeanor
☒ Felony

PENALTY: PLEASE SEE ATTACHMENT

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

DEFENDANT - U.S.

IVAN GENNADIEVICH KONDRATIEV

DISTRICT COURT NUMBER

CR22-201JST

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Federal Bureau of Investigation

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrP 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:
☐ U.S. ATTORNEY ☐ DEFENSE
SHOW
DOCKET NO.
☐ this prosecution relates to a pending case involving this same defendant

MAGISTRATE
CASE NO.
☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person
 Furnishing Information on this form STEPHANIE M. HINDS

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.
 Attorney (if assigned) Helen Gilbert

DEFENDANT**IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

1) ☒ If not detained give date any prior summons was served on above charges N/A

2) ☐ Is a Fugitive3) ☐ Is on Bail or R**IS IN CUSTODY**4) ☐ On this charge5) ☐ On another conviction6) ☐ Awaiting trial on other chargesIf answer to (6) is "Yes", show name of institution

Has detainer
 been filed? ☐ Yes ☒ No

If "Yes"
 give date
 filed _____

**DATE OF
 ARREST**

Month/Day/Year

Or... if Arresting Agency & Warrant were not

**DATE TRANSFERRED
 TO U.S. CUSTODY**

Month/Day/Year

FILED

May 17 2022

Mark B. Busby
 CLERK, U.S. DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO

☐ This report amends AO 257 previously submitted
ADDITIONAL INFORMATION OR COMMENTS**PROCESS:**
☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT
Bail Amount: no bail

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET

UNITED STATES V. IVAN GENNADIEVICH KONDRATIEV

Count One: 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B), and 2 – Obtaining Information from a Protected Computer and Aiding and Abetting

5 years imprisonment;
3 years supervised release;
\$250,000 fine; restitution; forfeiture; \$100 special assessment.

Count Two: 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B), and 2 – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer and Aiding and Abetting

10 years imprisonment;
3 years supervised release;
\$250,000 fine; restitution; forfeiture; \$100 special assessment

Count Three: 18 U.S.C. §§ 1030(a)(7)(A), (a)(7)(B), (a)(7)(C), and (c)(3)(A), and 2 – Extortion Involving Computers and Aiding and Abetting

5 years imprisonment;
3 years supervised release;
\$250,000 fine; restitution; forfeiture; \$100 special assessment

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: OAKLAND

FILED

May 17 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

IVAN GENNADIEVICH KONDRATIEV,
a/k/a Ivan Gennadyevich Kondratyev, a/k/a Ivan
Kondratyev, a/k/a Ivan Kondratiev, a/k/a Ivan
Kondratev, a/k/a Ivan Gennadyevich, a/k/a Bassterlord,
a/k/a FishEye, a/k/a ИВАН ГЕННАДЬЕВИЧ
КОНДРАТЬЕВ,

DEFENDANT(S).

INDICTMENT

18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B) – Obtaining Information from a Protected Computer;

18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B) – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer;

18 U.S.C. §§ 1030(a)(7)(A), (a)(7)(B), (a)(7)(C), (c)(3)(A) – Extortion Involving Computers;

18 U.S.C. § 2 – Aiding and Abetting;

18 U.S.C. §§ 982(a)(2)(B) and 1030(i) – Forfeiture Allegation

A true bill.

/s/ Foreperson of the Grand Jury

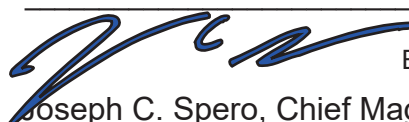
Foreman

Filed in open court this 17th day of

May, 2022



Clerk



Bail, \$ Arrest Warrant

Joseph C. Spero, Chief Magistrate Judge

FILED

May 17 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

STEPHANIE M. HINDS (CABN 154284)
United States Attorney

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

UNITED STATES OF AMERICA,)	CASE NO. CR22-201JST
Plaintiff,)	<u>VIOLATIONS:</u>
v.)	18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B) – Obtaining
)	Information from a Protected Computer;
IVAN GENNADIEVICH KONDRATIEV,)	18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B) – Transmission
a/k/a Ivan Gennadyevich Kondratyev,)	of a Program, Information, Code, and Command to
a/k/a Ivan Kondratyev,)	Cause Damage to a Protected Computer;
a/k/a Ivan Kondratiev,)	18 U.S.C. §§ 1030(a)(7)(A), (a)(7)(B), (a)(7)(C),
a/k/a Ivan Kondratev,)	(c)(3)(A) – Extortion Involving Computers;
a/k/a Ivan Gennadyevich,)	18 U.S.C. § 2 – Aiding and Abetting;
a/k/a Bassterlord,)	18 U.S.C. §§ 982(a)(2)(B) and 1030(i) – Forfeiture
a/k/a FishEye,)	Allegation
a/k/a ИВАН ГЕННАДЬЕВИЧ)	
КОНДРАТЬЕВ,)	OAKLAND VENUE
Defendant.)	

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. IVAN GENNADIEVICH KONDRATIEV, aka Ivan Gennadyevich Kondratyev, aka Ivan Kondratyev, aka Ivan Kondratiev, aka Ivan Kondratev, aka Ivan Gennadyevich, aka Bassterlord, aka FishEye, aka ИВАН ГЕННАДЬЕВИЧ КОНДРАТЬЕВ, was a Russian or Ukrainian national who lived

INDICTMENT

Overview

- a. Used various techniques and tools to hack into the computer network of Victim Company A;
- b. Copied and electronically transferred (or “exfiltrated”) data from Victim Company A’s networks;
- c. Encrypted data and computers on Victim Company A’s networks, using a form of malicious software called ransomware, with the objective of preventing Victim Company A from accessing and using data on the compromised computers; and
- d. Attempted to extort and extorted Victim Company A for a ransom payment in exchange for the decryption tool and key to unlock the compromised computers and for refraining from widely distributing Victim Company A’s stolen exfiltrated data.

Relevant Terms

5. Monero was a type of virtual currency, circulated over the Internet as a form of value. Monero was not issued by any government, bank, or company, but rather was generated and controlled through computer software operating via a decentralized, peer-to-peer network. Monero was just one of many varieties of virtual currency.

6. “Encryption” was the conversion of data into a secret code. In order to access encrypted data, a user had to have access to a password (known as a “decryption key”) or to a “decryptor” tool that enabled the user to decrypt the data. By encrypting files on a system, a cybercriminal could make the files unreadable and unusable until the files were decrypted.

7. “Malware” was malicious computer software, installed on a victim’s computer without authorization, that was intended to cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer.

8. “Ransomware” was a type of malware that infected a victim’s computer and encrypted some or all of the data on the computer. In some instances, ransomware, used in combination with other attack tools (collectively referred to as “ransomware”), also caused the victim’s data to be copied and electronically transferred (exfiltrated) from the victim’s computer network to servers under the control of the cybercriminals, all without authorization. Cybercriminals typically extorted the victim by demanding that the victim pay a ransom in order to decrypt and recover the data on the victim’s computer. Cybercriminals also extorted the victim by threatening to publish and/or distribute the victim’s stolen exfiltrated data if the victim refused to pay the ransom.

9. A “server” was a type of computer or device on a network that managed network resources.

COUNT ONE: (18 U.S.C. §§ 1030(a)(2)(C), (c)(2)(B), and 2 – Obtaining Information from a Protected Computer and Aiding and Abetting)

10. Paragraphs 1 through 9 of this Indictment are re-alleged and incorporated as if fully set forth here.

11. Beginning at a date unknown, but by on or about August 29, 2020, and continuing through on or about September 3, 2020, in the Northern District of California and elsewhere, the defendant,

IVAN GENNADIEVICH KONDRATIEV,
a/k/a Ivan Gennadyevich Kondratyev,
a/k/a Ivan Kondratyev,
a/k/a Ivan Kondratiev,
a/k/a Ivan Kondratev,
a/k/a Ivan Gennadyevich,
a/k/a Bassterlord,
a/k/a FishEye,

a/k/a ИВАН ГЕННАДЬЕВИЧ КОНДРАТЬЕВ,

intentionally accessed a protected computer without authorization and aided and abetted such access, and thereby obtained information from a protected computer, and committed the offense for purposes of commercial advantage and private financial gain, and committed the offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States and any state, and the value of the information obtained exceeded \$5,000; specifically, defendant accessed and aided and abetted the access of one or more computers of Victim Company A, which were located in the Northern District of California, and exfiltrated data, all without authorization, all in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), (ii), (iii), and 2.

COUNT TWO: (18 U.S.C. §§ 1030(a)(5)(A), (c)(4)(B), and 2 – Transmission of a Program, Information, Code, and Command to Cause Damage to a Protected Computer and Aiding and Abetting)

12. Paragraphs 1 through 9 of this Indictment are re-alleged and incorporated as if fully set forth here.

13. Beginning at a date unknown, but by on or about August 29, 2020, and continuing through on or about September 3, 2020, in the Northern District of California and elsewhere, the defendant,

IVAN GENNADIEVICH KONDRATIEV,
a/k/a Ivan Gennadyevich Kondratyev,
a/k/a Ivan Kondratyev,
a/k/a Ivan Kondratiev,
a/k/a Ivan Kondratev,
a/k/a Ivan Gennadyevich,
a/k/a Bassterlord,
a/k/a FishEye,
a/k/a ИВАН ГЕННАДЬЕВИЧ КОНДРАТЬЕВ,

knowingly caused and aided and abetted the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit, the defendant caused and aided and abetted the transmission of ransomware to one or more computers of Victim Company A, which were located in the Northern District of California and were used in interstate and foreign commerce and communication, and, by such conduct, caused loss to one or more persons during a one-year period aggregating at least \$5,000 in value, all in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and 2.

COUNT THREE: (18 U.S.C. §§ 1030(a)(7)(A), (a)(7)(B), (a)(7)(C), (c)(3)(A), and 2 – Extortion Involving a Protected Computer and Aiding and Abetting)

14. Paragraphs 1 through 9 of this Indictment are re-alleged and incorporated as if fully set forth here.

15. Beginning on or about August 29, 2020, and continuing through on or about September 3, 2020, in the Northern District of California and elsewhere, the defendant,

IVAN GENNADIEVICH KONDRATIEV,
a/k/a Ivan Gennadyevich Kondratyev,
a/k/a Ivan Kondratyev,
a/k/a Ivan Kondratiev,
a/k/a Ivan Kondratev,
a/k/a Ivan Gennadyevich,
a/k/a Bassterlord,
a/k/a FishEye,
a/k/a ИВАН ГЕННАДЬЕВИЧ КОНДРАТЬЕВ,

knowingly and with intent to extort from any person, specifically, Victim Company A, any money or thing of value, transmitted in interstate and foreign commerce, and aided and abetted such transmission, any communication containing a threat to cause damage to a protected computer, a threat to impair the confidentiality of information obtained from a protected computer without authorization, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, all in violation of Title 18, United States Code, Sections 1030(a)(7)(A), (a)(7)(B), (a)(7)(C), (c)(3)(A), and 2.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(2)(B) and 1030(i))

16. The allegations contained in this Indictment are re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

17. Upon conviction for the offenses set forth in Count One through Three in violation of Title 18, United States Code, Section 1030(a), set forth in this Indictment, the defendant,

IVAN GENNADIEVICH KONDRATIEV,
a/k/a Ivan Gennadyevich Kondratyev,
a/k/a Ivan Kondratyev,
a/k/a Ivan Kondratiev,
a/k/a Ivan Kondratev,
a/k/a Ivan Gennadyevich,
a/k/a Bassterlord,
a/k/a FishEye,

1 a/k/a ИВАН ГЕННАДЬЕВИЧ КОНДРАТЬЕВ,

2 shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and
3 1030(i), any personal property used or intended to be used to commit or to facilitate the commission of
4 said violation or a conspiracy to violate said provision, and any property, real or personal, which
5 constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of
6 money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from
7 the violation, or the value of the property used to commit or to facilitate the commission of said
8 violation.

9 If any of the property described above, as a result of any act or omission of the defendant:

- 10 a. cannot be located upon exercise of due diligence;
11 b. has been transferred or sold to, or deposited with, a third party;
12 c. has been placed beyond the jurisdiction of the court;
13 d. has been substantially diminished in value; or
14 e. has been commingled with other property which cannot be divided without
15 difficulty,

16 the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21,
17 United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 1030(i)(2).

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

1 All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, and Federal Rule
2 of Criminal Procedure 32.2.

3
4 DATED: May 17, 2022

A TRUE BILL.

5
6 s/Foreperson
FOREPERSON

7
8 STEPHANIE M. HINDS
9 United States Attorney

10 s/Helen L. Gilbert
11 HELEN L. GILBERT
12 Assistant United States Attorney